UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/714,082	11/16/2000	Lewis T. Donzis	NORR0007US(12514RXUS02U)	5132

21906 7590 12/14/2004

TROP PRUNER & HU, PC
8554 KATY FREEWAY
SUITE 100
HOUSTON, TX 77024

EXAMINER	
LAZARO, DAVID R	

ART UNIT	PAPER NUMBER
2155	

DATE MAILED: 12/14/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/714,082	DONZIS ET AL.	
	Examiner	Art Unit	
	David Lazaro	2155	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 November 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-10,12,13,16,17,19-26,28-30 and 32-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-10,12,13,16,17,19-26,28-30 and 32-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to the RCE filed 11/10/04.

2. Claims 40-43 were added.

3. Claims 2-10, 12, 13, 16, 17, 19-26, 28-30 and 32-43 are pending in this Office Action.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 41-43 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Claims 41-43 each contain the limitation "wherein the ping message is according to a protocol defining a layer higher than layer 2". While support is present for a ping message defined outside the security protocol used in a secure link, there is no support in the specification for limiting the ping message protocol to a layer higher than layer 2. It is not supported in the general context of the specification, and there is no antecedent basis from the specification for the claim language presented in these claims. For these reasons, Claims 41-43 fail to comply with the written description requirement.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 2, 3, 6, 7, 8, 12, 13, 19-23, 28, 30 and 32-39 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,473,798 by Grosser.

8. With respect to Claim 32, Grosser teaches a method of determining if a link is alive (Col. 1 lines 8-14), comprising: establishing a secure link (Col. 1 lines 33-55) between a first node (Col. 3 lines 22-33) and a second node (Col. 3 lines 46-49) according to a security protocol (Col. 4 lines 23-28); sending at least one ping message targeting the second node over the secure link (Col. 6 lines 34-60), the at least one ping message defined outside the security protocol (Col. 6 lines 53-60); and monitoring for at least one ping reply to determine if the secure link is alive (Col. 6 line 61 – Col. 7 line 8) wherein sending the at least one ping message comprises sending the at least one ping message protected according to the security protocol (Col. 4 lines 23-28).

9. With respect to Claim 33, Grosser teaches all the limitations of Claim 32 and further teaches the security protocol comprises an Internet Protocol Security protocol (IPsec) (Col. 4 lines 23-38), and wherein sending the at least one ping message comprises sending the at least one ping message encrypted according to an IPsec

security association (This would be inherent in the use of IPsec with L2TP as stated in Col. 4 lines 23-28).

10. With respect to Claim 40, Grosser teaches all the limitations of Claim 33 and further teaches, wherein the ping message is defined according to a protocol outside IPsec (Col. 6 lines 53-60).

11. With respect to Claim 2, Grosser teaches all the limitations of Claim 32 and further teaches establishing the secure link comprises establishing a virtual private network session (Col. 1 lines 33-41).

12. With respect to Claim 3, Grosser teaches all the limitations of Claim 32 and further teaches establishing the secure link comprises establishing a link protected by an Internet Protocol Security protocol (Col. 4 lines 23-28).

13. With respect to Claim 6, Grosser teaches all the limitations of Claim 32 and further teaches establishing the secure link comprises establishing the secure link between first and second nodes each comprising a security gateway (Col. 3 lines 23-28 and lines 34-39).

14. With respect to Claim 7, Grosser teaches all the limitations of Claim 6 and further teaches sending at least one ping message targeting another node behind the second node (Col 6 lines 37-51).

15. With respect to Claim 8, Grosser teaches all the limitations of Claim 7 and further teaches monitoring for at least one ping reply from the other node (Col. 6 line 61 – Col. 7 line 8).

16. With respect to Claim 34, Grosser teaches a method of communicating with a remote node (Col. 1 lines 8-14 and Col. 3 lines 46-49), comprising: establishing a secure link (Col. 1 lines 33-55 and Col. 4 lines 23-28) between a first security gateway (Col. 3 lines 23-28) and a second security gateway (Col. 3 lines 34-39), the remote node in communication with the second security gateway; sending at least one ping message to the remote node over the secure link and through the second security gateway (Col. 6 lines 34-60); and monitoring for at least one ping reply from the remote node to determine if the secure link is alive (Col. 6 line 61 – Col. 7 line 8), wherein establishing the secure link comprises establishing a secure link protected according to a security protocol (Col. 4 lines 23-28), wherein sending the at least one ping message comprises sending at least one ping message defined outside the security protocol (Col. 6 lines 53-60), wherein sending the at least one ping message comprises sending the at least one ping message protected according to the security protocol (Col. 4 lines 23-28).

17. With respect to Claim 35, Grosser teaches all the limitations of Claim 34 and further teaches the security protocol comprises an Internet Protocol Security protocol (IPsec) (Col. 4 lines 23-38), and wherein sending the at least one ping message comprises sending the at least one ping message encrypted according to an IPsec security association (This would be inherent in the use of IPsec in conjunction with L2TP as stated in Col. 4 lines 23-28).

18. With respect to Claim 12, Grosser teaches all the limitations of Claim 34 and further teaches establishing a secure link comprises establishing a secure link protected by an Internet Protocol Security protocol (Col. 4 lines 23-28).

19. With respect to Claim 13, Grosser teaches all the limitations of Claim 34 and further teaches establishing the secure link comprises establishing a virtual private network session (Col. 1 lines 33-41).

20. With respect to Claim 36, Grosser teaches a system for communicating (Col. 1 lines 8-14) between a network element and a remote node (Col. 3 lines 46-49), comprising: a security module adapted to establish a secure link with the remote node, the secure link (Col. 1 lines 33-55), having a security mechanism according to a security protocol (Col. 4 lines 23-28); and a keep-alive module adapted to send at least one ping message over the secure link to the remote node (Col. 6 lines 34-60), the at least one ping message defined outside the security protocol (Col. 6 lines 53-60), sending the at least one ping message comprises sending the at least one ping message protected according to the security protocol (Col. 4 lines 23-28).

21. With respect to Claim 37, Grosser teaches all the limitations of Claim 36 and further teaches the security protocol comprises an Internet Protocol Security protocol (IPsec) (Col. 4 lines 23-38), and wherein sending the at least one ping message comprises sending the at least one ping message encrypted according to an IPsec security association (This would be inherent in the use of IPsec in conjunction with L2TP as stated in Col. 4 lines 23-28).

22. With respect to Claim 19, Grosser teaches all the limitations of Claim 36 and further teaches the security protocol comprises an Internet Protocol Security Protocol (Col. 4 lines 23-28).

23. With respect to Claim 21, Grosser teaches all the limitations of Claim 36 and further teaches an interface to a packet-based network, the secure link established over the packet-based network; and a layer to control communications over the packet-based network (Col. 1 lines 16-42 and lines 43-48).

24. With respect to Claim 22, Grosser teaches all the limitations of Claim 21 and further teaches the layer comprises an Internet Protocol layer (Col. 1 lines 16-21).

25. With respect to Claim 23, Grosser teaches all the limitations of Claim 36 and further teaches the keep-alive module is adapted to further monitor for at least one ping reply responsive to the at least one ping message to determine if the secure link is alive (Col. 6 line 61 – Col. 7 line 8).

26. With respect to Claim 38, Grosser teaches an article comprising at least one storage medium containing instructions for controlling communications (Col. 7 lines 20-47), the instructions when executed causing a controller to: establish a secure link (Col. 1 lines 33-55) between a first node (Col. 3 lines 22-33) and a second node (Col. 3 lines 46-49) according to a security protocol (Col. 4 lines 23-28); send at least one ping message targeting the second node over the secure link (Col. 6 lines 34-60), the at least one ping message defined outside the security protocol (Col. 6 lines 53-60); and monitor for at least one ping reply to determine if the secure link is alive (Col. 6 line 61 – Col. 7 line 8), wherein sending the at least one ping message comprises sending the at least one ping message protected according to the security protocol (Col. 4 lines 23-28).

27. With respect to Claim 39, Grosser teaches all the limitations of Claim 38 and further teaches the security protocol comprises an Internet Protocol Security protocol

(IPsec) (Col. 4 lines 23-38), and wherein sending the at least one ping message comprises sending the at least one ping message encrypted according to an IPsec security association (This would be inherent in the use of IPsec in conjunction with L2TP as stated in Col. 4 lines 23-28).

28. With respect to Claim 28, Grosser teaches all the limitations of Claim 38 and further teaches the instructions when executed cause the controller to further establish an Internet Protocol security association for the secure link (Col. 4 lines 23-28).

29. With respect to Claim 30, Grosser teaches all the limitations of Claim 38 and further teaches the controller is part of the first node (Col. 5 lines 24-28).

Claim Rejections - 35 USC § 103

30. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

31. Claims 5, 20, 4, 16, 17 and 41-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grosser in view of U.S. Patent 6,182,226 by Reid et al. (Reid).

32. With respect to Claim 5, Grosser teaches a method of determining if a link is alive (Col. 1 lines 8-14), comprising: establishing a secure link (Col. 1 lines 33-55) between a first node (Col. 3 lines 22-33) and a second node (Col. 3 lines 46-49) according to a security protocol (Col. 4 lines 23-28); sending at least one ping message targeting the second node over the secure link (Col. 6 lines 34-60), the at least one ping

message defined outside the security protocol (Col. 6 lines 53-60); and monitoring for at least one ping reply to determine if the secure link is alive (Col. 6 line 61 – Col. 7 line 8). Grosser does not explicitly disclose sending a ping message comprising sending at least one Internef Control Message Protocol (ICMP) message. Reid teaches sending a ping message may comprise sending at least one ICMP message (Col. 15 lines 59-61). It would have been obvious to one of ordinary skill in the art at the time the invention was made to take the method disclosed by Grosser and modify it as indicated by Reid such that sending the at least one ping message comprises sending at least one Internet Control Message Protocol message. One would be motivated to have this since it is a "commonly known" way to send a ping message and could therefore be more easily incorporated into existing systems (Col. 15 lines 59-61 of Reid).

33. With respect to Claim 20, teaches a system for communicating (Col. 1 lines 8-14) between a network element and a remote node (Col. 3 lines 46-49), comprising: a security module adapted to establish a secure link with the remote node, the secure link (Col. 1 lines 33-55), having a security mechanism according to a security protocol (Col. 4 lines 23-28); and a keep-alive module adapted to send at least one ping message over the secure link to the remote node (Col. 6 lines 34-60), the at least one ping message defined outside the security protocol (Col. 6 lines 53-60). Grosser does not explicitly disclose the ping message comprising an Internet Control Message Protocol (ICMP) message. Reid teaches a ping message may comprise a ICMP message (Col. 15 lines 59-61). It would have been obvious to one of ordinary skill in the art at the time the invention was made to take the system disclosed by Grosser and modify it as

indicated by Reid such that the at least one ping message comprises an Internet Control Message Protocol message. One would be motivated to have this since it is a "commonly known" way to send a ping message and could therefore be more easily incorporated into existing systems (Col. 15 lines 59-61 of Reid).

34. With respect to Claim 4, Grosser teaches all the limitations of Claim 3 but does not explicitly disclose sending a ping message comprising sending at least one Internet Control Message Protocol (ICMP) message. Reid teaches sending a ping message may comprise sending at least one ICMP message (Col. 15 lines 59-61). It would have been obvious to one of ordinary skill in the art at the time the invention was made to take the method disclosed by Grosser and modify it as indicated by Reid such that sending the at least one ping message comprises sending at least one Internet Control Message Protocol message. One would be motivated to have this since it is a "commonly known" way to send a ping message and could therefore be more easily incorporated into existing systems (Col. 15 lines 59-61 of Reid).

35. With respect to Claim 16, Grosser teaches all the limitations of Claim 34 but does not explicitly disclose sending a ping message comprising sending at least one Internet Control Message Protocol (ICMP) message. Reid teaches sending a ping message may comprise sending at least one ICMP message (Col. 15 lines 59-61). It would have been obvious to one of ordinary skill in the art at the time the invention was made to take the method disclosed by Grosser and modify it as indicated by Reid such that sending the at least one ping message comprises sending at least one Internet Control Message Protocol message. One would be motivated to have this since it is a

"commonly known" way to send a ping message and could therefore be more easily incorporated into existing systems (Col. 15 lines 59-61 of Reid).

36. With respect to Claim 17, Grosser in view of Reid teaches all the limitations of Claim 16 and further teaches establishing a secure link comprises establishing a secure link according to an Internet Protocol Security protocol (Col. 4 lines 23-28 of Grosser).

37. With respect to Claim 41, Grosser teaches all the limitations of Claim 32 and further teaches the use of a generic ping message in determining if a link is alive (Col. 6 lines 30-52). Grosser does not explicitly state the specific use of a ping message according to a protocol defining a layer higher than layer 2. However, Reid teaches the use of a ping message according to the Internet Control Message Protocol (ICMP). ICMP is a protocol in a layer higher than layer 2. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made, to take the method of Grosser and modify it as indicated by Reid such that the ping message is according to a protocol defining a layer higher than layer 2. One would be motivated to have this since the use of ICMP messages is a "commonly known" way to send a ping message and could therefore be more easily incorporated into existing systems (Col. 15 lines 59-61 of Reid).

38. With respect to Claim 42, Grosser teaches all the limitations of Claim 34 and further teaches the use of a generic ping message in determining if a link is alive (Col. 6 lines 30-52). Grosser does not explicitly state the specific use of a ping message according to a protocol defining a layer higher than layer 2. However, Reid teaches the use of a ping message according to the Internet Control Message Protocol (ICMP).

ICMP is a protocol in a layer higher than layer 2. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made, to take the method of Grosser and modify it as indicated by Reid such that the ping message is according to a protocol defining a layer higher than layer 2. One would be motivated to have this since the use of ICMP messages is a "commonly known" way to send a ping message and could therefore be more easily incorporated into existing systems (Col. 15 lines 59-61 of Reid).

39. With respect to Claim 43, Grosser teaches all the limitations of Claim 36 and further teaches the use of a generic ping message in determining if a link is alive (Col. 6 lines 30-52). Grosser does not explicitly state the specific use of a ping message according to a protocol defining a layer higher than layer 2. However, Reid teaches the use of a ping message according to the Internet Control Message Protocol (ICMP). ICMP is a protocol in a layer higher than layer 2. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made, to take the system of Grosser and modify it as indicated by Reid such that the ping message is according to a protocol defining a layer higher than layer 2. One would be motivated to have this since the use of ICMP messages is a "commonly known" way to send a ping message and could therefore be more easily incorporated into existing systems (Col. 15 lines 59-61 of Reid).

40. Claims 9, 10, 24, 25 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grosser in view of U.S. Patent 6,636,898 by Ludovici et al. (Ludovici).

41. With respect to Claim 9, Grosser teaches all the limitations of Claim 32. Although Grosser teaches remedial action may occur to correct a link that is not alive (Col. 5 lines 9-12), Grosser does not explicitly disclose tearing down the secure link if it is determined to not be alive. Ludovici teaches that in a VPN using a secure link, such as those using IPSec protocol (Col. 1 lines 49-52), the link should be torn down when errors concerning the link are detected (Col. 1 line 57 – Col. 2 line 10). It would have been obvious to one of ordinary skill in the art at the time the invention was made to take the method of Grosser and modify it as indicated by Ludovici such that the method further comprises tearing down the secure link if the secure link is determined not to be alive. One would be motivated to have this as it ensures the system is not compromised and enables more efficient management of connection lifetimes and security associations (Col. 1 line 57 – Col. 2 line 10 of Ludovici).

42. With respect to Claim 10, Grosser in view of Ludovici teaches all the limitations of Claim 9 and further teaches tearing down the secure link comprises tearing down a security association according to an Internet Protocol Security protocol (Col. 1 lines 49-51 and Col. 5 lines 30-36 of Ludovici).

43. With respect to Claim 24, Grosser teaches all the limitations of Claim 23. Grosser teaches remedial action may occur to correct a link that is not alive (Col. 5 lines 9-12), but does not explicitly disclose the security module being adapted to tear down a

security association of a secure link if it is not alive. Ludovici teaches that in a VPN using a secure link, such as those using IPSec protocol (Col. 1 lines 49-52), the link and its security associations (Col. 1 lines 49-51 and Col. 5 lines 30-36) should be torn down when errors concerning the link are detected (Col. 1 line 57 – Col. 2 line 10). It would have been obvious to one of ordinary skill in the art at the time the invention was made to take the system of Grosser and modify it as indicated by Ludovici such that the security module is adapted to tear down a security association of the secure link if the secure link is not alive. One would be motivated to have this as it ensures the system is not compromised and enables more efficient management of connection lifetimes and security associations (Col. 1 line 57 – Col. 2 line 10 of Ludovici).

44. With respect to Claim 25, Grosser in view of Ludovici teaches all the limitations of Claim 24 and further teaches the security association comprises an Internet Protocol Security protocol security association (Col. 1 lines 49-52 of Ludovici).

45. With respect to Claim 29, Grosser teaches all the limitations of Claim 28. Grosser teaches remedial action may occur to correct a link that is not alive (Col. 5 lines 9-12), but does not explicitly disclose tearing down the security association if the controller does not receive the at least one ping reply. Ludovici teaches that in a VPN using a secure link, such as those using IPSec protocol (Col. 1 lines 49-52), the link and its security associations (Col. 1 lines 49-51 and Col. 5 lines 30-36) should be torn down when errors concerning the link are detected (Col. 1 line 57 – Col. 2 line 10). It would have been obvious to one of ordinary skill in the art at the time the invention was made to take the system of Grosser and modify it as indicated by Ludovici such that the

instructions when executed cause the controller to tear down the security association if the controller does not receive the at least one ping reply. One would be motivated to have this as it ensures the system is not compromised and enables more efficient management of connection lifetimes and security associations (Col. 1 line 57 – Col. 2 line 10 of Ludovici).

46. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Grosser in view of U.S. Patent 6,173,411 by Hirst et al. (Hirst). Grosser teaches all the limitations of Claim 36 and further teaches the keep-alive module is adapted to further monitor for at least one ping reply responsive to the at least one ping message to determine if the secure link is alive (Col. 6 line 61 – Col. 7 line 8). Although Grosser teaches remedial action may occur to correct a link that is not alive (Col. 5 lines 9-12), Grosser does not explicitly disclose establishing a link over a secondary communication network if the secure link is not alive. However, Hirst teaches that upon detecting a link is not alive, one can establish a link over a secondary communication network (Col. 2 line 54 – Col. 3 line 13). It would have been obvious to one of ordinary skill in the art at the time the invention was made to take the system disclosed by Grosser and modify it as indicated by Hirst such that the system further comprises a module adapted to establish a link over a secondary communication network if the secure link is not alive. One would be motivated to have this since the reliability of a network connection is a critical concern (Col. 1 lines 20-35).

Response to Arguments

47. Applicant's arguments filed 11/10/04 have been fully considered but they are not persuasive.

48. Applicants first set of arguments focus on the claim language regarding "wherein sending the at least one ping message comprises sending the at least one ping message protected according to the security protocol". The applicants generally state,

> *"It is respectfully submitted that the Layer 2 test packet (L2TP Hello, L2F ECHO, or PTP Echo-Request) as taught by Grosser cannot be protected according to a security protocol, as recited in claim 32."*

The examiner will first address the issue regarding network layers in regards to communications over a Layer 2 tunnel such as a L2TP tunnel.

49. Applicants make numerous arguments regarding the issue of network layers such as "*Encrypting a lower level test packet, such as a Layer 2 test packet, using a higher level security protocol, such as IPsec, does not make much practical sense*" (Page 10 of Remarks, end of 1st paragraph), "*For a Layer 2 test packet to be protected by IPsec, as suggested by the Office Action, the L2TP layer (layer 2) would have to be provided above the IPsec layer (Layer 3), which is clearly prohibited*" (Page 10 of remarks, end of 2nd paragraph), and "*For a layer 2 test packet to be encapsulated in a UDP packet, layer 2 will have to be provided above layer 4, which is clearly erroneous*" (Page 10 of Remarks, end of 3rd paragraph). Applicants rely on "Introduction to Internet" for explaining why these arguments are valid based on the Open System Interconnection (OSI) reference model. However, as stated on page 4 of "Introduction to Internet", "The OSI reference model is a conceptual model composed of seven

layers, each specifying particular network functions...it is now considered the primary architectural model for intercomputer communications" (Emphasis added). The OSI reference model, as the name suggests, is a model, not an actual way of communicating. This is better said on Page 5 of "Introduction to Internet", under 'Protocols', which states, "The OSI model provides a conceptual framework for communication between computers, but the model itself is not a method of communication. Actual communication is made possible by using communication protocols." As such, the basis of the Examiner's responses relies on analysis and specific teachings of the protocols used in the cited prior. The key points of the Applicants' arguments will now be addressed.

50. Applicants argue - "*As expressly taught by Grosser, the three Layer 2 tunnels discussed above do not themselves specify or provide data security." Grosser, 4:23-24. In other words, the Layer 2 test packets sent in Layer 2 tunnels described in Grosser are not protected according to a security protocol... The column 4, lines 23-28, passage of Grosser refers to using PPP or IPsec packet encryption in conjunction with a Layer 2 VPN tunnel link to provide packet security between tunnel endpoints. This passage refers to protecting data packets that are sent through the IPsec layer. However, nowhere in Grosser is there any indication that the Layer 2 test packets are themselves protected by IPsec.*"

a. Column 4, lines 23-28 of Grosser does indeed discuss the use of IPsec protocol encryption for security of packets sent between tunnel endpoints. It is reasonable to conclude from Grosser's statement of providing "packet security at least between endpoints", that Layer 2 test packets would be included and can be protected by IPsec when used in conjunction with a Layer 2 tunnel such as a

L2TP tunnel. Grosser does not state Layer 2 test packets would be excluded from protection if IPsec were used.

Furthermore, as mention in the advisory action, RFC 2661 (provided by Applicants in the IDS submitted 02/12/04), which is the standard for the Layer 2 Tunneling Protocol (L2TP), provides explicit statements of protecting an entire L2TP packet. Section 9.2 states "Securing L2TP requires that the underlying transport make available encryption, integrity and authentication services for all L2TP traffic. This secure transport operates on the entire L2TP packet and is functionally independent of PPP and the protocol being carried by PPP" (emphasis added). Section 9.4, titled "L2TP and IPsec", further states "When running over IP, IPsec provides packet-level security via ESP and/or AH. All L2TP control and data packets for a particular tunnel appear as homogeneous UDP/IP data packets to the IPsec system." Based on these 2 statements, an entire L2TP control or data packet would be protected through IPsec.

For these reasons, a Layer 2 test packet can be protected according to a security protocol such as IPsec. Therefore, the teachings of Grosser are within the scope of "wherein sending the at least one ping message comprises sending the at least one ping message protected according to the security protocol".

51. Applicants argue - "*For a Layer 2 test packet to be protected by IPsec, as suggested by the Office Action, the L2TP layer (layer 2) would have to be provided above the IPsec layer (Layer 3), which is clearly prohibited*"

b. As initially discussed, the OSI reference model, as explained in "Introduction to Internet", provides a conceptual model while the protocols provide the actual communication methods. As discussed above, RFC 2661 clearly allows L2TP packets to be protected through IPsec. This includes encryption of the header and associated PPP information being carried. As further evidence of IPsec being used in conjunction with L2TP, see Page 25-28 of "Layer 2 Tunneling Protocol (L2TP) Overview" by the IBM Corporation. Specifically, page 28 states,

> "The IPSec protocols Authentication Header (AH) and/or Encapsulated Security Payload (ESP) can be used to protect a L2TP tunnel. There are slight differences in the protection level, depending on the tunnel mode used. In the voluntary mode, all the traffic including the L2TP and virtual PPP header is protected by IPSec. In the compulsory mode, all traffic is protected except the PPP header between the remote client and the ISP."

For these reasons, a Layer 2 test packet can be protected by IPsec. Therefore, the teachings of Grosser are within the scope of "wherein sending the at least one ping message comprises sending the at least one ping message protected according to the security protocol".

52. Applicants argue - "*The statement made by the Advisory Action that an L2TP packet is encapsulated in a UDP packet is erroneous. UDP (or TCP) is layer 4, which is two layers higher than layer 2. See "Introduction to Internet" p. 6. For a layer 2 packet to*

be encapsulated in a UDP packet, layer 2 will have to be provided above layer 4, which is clearly erroneous."

c. As initially discussed, the OSI reference model, as explained in "Introduction to Internet", provides a conceptual model while the protocols provide the actual communication methods. As such, one of the primary functions of L2TP is to tunnel PPP frames (See the Introduction in RFC 2661). RFC 2661 explicitly states in section 3.0, 'Protocol Overview', "PPP Frames are passed over an unreliable Data Channel encapsulated first by an L2TP header and then a Packet Transport such as UDP, Frame Relay, ATM, etc." The L2TP packet includes the header and the PPP frame as a payload. The L2TP is further encapsulated by UDP if the network is an IP network. In RFC 2661, section 8.1, 'L2TP over UDP/IP', it further states, "L2TP uses the registered UPD port 1701 [RFC 1700]. The entire L2TP packet, including payload and L2TP header, is sent within a UDP datagram." Both of these citations explicitly state an L2TP packet is encapsulated in a UDP packet. Therefore, the statement made in the Advisory Action is not erroneous.

53. Applicants argue - "*There simply did not exist any reason to incorporate the teachings of Reid regarding ICMP ping messages into the Layer 2 tunnel testing mechanism of Grosser. As discussed above, the focus of Grosser is on testing Layer 2 tunnels with Layer 2 test packets. Using a higher level ping message in place of the Layer 2 test packets would render the Grosser mechanism inoperative for its intended purpose. It is respectfully submitted that an ICMP ping message, as taught by Reid, cannot be used to test a Layer 2 tunnel, which is the focus of the teachings of Grosser.*"

d. As initially discussed, the OSI reference model, as explained in "Introduction to Internet", provides a conceptual model while the protocols provide the actual communication methods. As such, one of the primary functions of L2TP is to tunnel PPP frames (See the Introduction in RFC 2661). As stated in the applicants specification on page 8, last paragraph, "PPP, as described in RFC 1661, entitled "The Point-to- Point Protocol (PPP)," dated July 1994, provides a standard method for transporting multi-protocol packets over point-to-point connections." This method of transporting multi-protocol packets includes functionality for an IP datagram payload. The IP datagram can include protocols in the TCP/IP family, which includes ICMP. Since a PPP frame can transport an IP datagram that can be an ICMP ping message, and a L2TP tunnels PPP frames, using a ICMP ping message would not render the Grosser mechanism inoperative for it intended purpose. As such, an ICMP ping message would be a reasonable test packet as it is commonly known, as suggested by Reid (Col. 15 lines 59-61) and as known in the art in general, for testing "connectivity and responsiveness" between two endpoints, which can include the endpoints of a layer 2 tunnel.

54. Applicants argue - "*The Advisory Action stated that the "Grosser teachings are open ended in terms of a protocol used for a test packet (Co1. 6 lines 30-60)." The cited column 6 passage of Grosser lists several alternative test messages for layer 2 - no suggestion is provided that a higher layer test message can be used.*"

e. The Advisory Action states "A preferred embodiment is stated as using layer 2 packets corresponding to the actual type of layer 2 tunnel, however, Grosser teachings are open ended in terms of a protocol used for a test packet (Col. 6 lines 30-60)." In lines 30-52, Grosser teaches the general process of determining when a to run a responsiveness test (a test do determine if the link is alive). Grosser generally refers to "sending a test packet to the specified host via a Layer 2 tunnel." (emphasis added). In lines 53-60, preferable "test packets" are listed that are associated to the type of Layer 2 tunnel. However, there is no statement in the Grosser reference indicating that other types of "test packets" are not allowable. The Examiner therefor asserts that Grosser's teachings are open ended in terms of a protocol used for a test packet.

55. Applicants argue - "*The Office Action has failed to establish that there would have been a reasonable expectation of success in using the ICMP ping messages of Reid in testing Layer 2 tunnels of Grosser. See M.P.E.P. § 2143, at 2100-129 ("[T]here must be a reasonable expectation of success."). It is highly unlikely that an ICMP message associated with a higher-level protocol can be used to successfully test a Layer 2 tunnel. More fundamentally, as Layer 2 test packets are available for testing Layer 2 tunnels, there would have been absolutely no reason whatsoever to employ a different level message, such as the ICMP ping message, to test the Layer 2 tunnels described in Grosser.*"

f. MPEP 2143.02 primarily deals with the Chemical and Biotechnology arts where there is an inherent level of unpredictability. The Electrical and Computer arts have a high level of predictability. MPEP 2143.02 also states that in predictable arts, the burden is on the applicant to show evidence that there was

no reasonable expectation of success. Applicants have failed to show sufficient evidence of there being no reasonable expectation of success. Only conclusive statements were given without specific evidence. Although the Applicants may be implying the previous arguments provide sufficient evidence to support their conclusion, the Examiner has already addressed these previous arguments. As such, the Examiner believes there is reasonable expectation of success based on the prior art of record both cited in the rejection and discussed in the Examiner's responses above.

Conclusion

56. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

57. "Introduction to Internet" - Originally cited in the Applicant's Remarks submitted 11/10/04. Also cited by Examiner in the response to arguments. Was not forwarded to the Examiner with the amendment so it is being made part of the record with this Office Action.

58. "Layer 2 Tunneling Protocol (L2TP) Overview" by the IBM Corporation, 1999, as printed from
www-1.ibm.com/servers/eserver/iseries/tcpip/vpn/redbooks/l2tppres/pdf/l2tppres.pdf
Used as evidence in Examiner's response to arguments. Discloses L2TP encapsulation and the use of IPsec with L2tp.

59. "Securing L2TP using IPSEC" INTERNET-DRAFT, October 1999,

<draft-ietf-pppext-l2tp-security-05.txt> Discloses a broad overview of the requirements and guidelines for the use of IPSec with L2TP.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to David Lazaro whose telephone number is 571-272-3986. The examiner can normally be reached on 8:30-5:00 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hosain Alam can be reached on 571-272-3978. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

David Lazaro
December 3, 2004

HOSAIN ALAM
SUPERVISORY PATENT EXAMINER